Two-server Password authenticated Key Exchange Protocol Based on MLWE

Yeming Yang
Information Engineering University
Zhengzhou, Henan, China
18888928280@163.com

Shuaichao Song
Information Engineering University
Zhengzhou, Henan, China
625262263@qq.com

Songhui Guo*
Information Engineering University
Zhengzhou, Henan, China
1157565763@qq.com

Abstract

Currently, PAKE (Password Authenticated Key Exchange) protocols on lattice using a single-server architecture are widely applied. However, such protocols are vulnerable to server leakage attacks, dictionary attacks, and other threats. To address these issues, researchers have proposed multi-server and two-server architecture-based PAKE protocols. However, PAKE protocols in a multi-server architecture require the use of complex cryptographic primitives such as signatures, and zero-knowledge proofs to ensure security, which reduces the execution efficiency of the protocol. To solve these problems, we propose a two-server PAKE protocol on the lattice based on the MLWE (Module learning with errors) problem. The protocol is built using instances of the MLWE problem and utilizes the Peikert error coordination technique, which ensures both parties with similar values arrive at the same result through computation. Additionally, we introduce the error pairing hypothesis and demonstrates its security within the random oracle model. The protocol securely stores different shares of password information across various servers. This approach protects user password data, even if one of the servers is compromised. Compared to similar protocols, we avoid the use of numerous cryptographic primitives, and can better resist quantum computing attacks and server leakage. And we reduce computational and communication costs, and can better meet practical application needs.

CCS Concepts

• **Security and privacy** → Security services; Authentication.

Keywords

two-server, MLWE, password authentication, key exchange

ACM Reference Format:
Yeming Yang, Shuaichao Song, and Songhui Guo. 2025. Two-server Password authenticated Key Exchange Protocol Based on MLWE. In *2025 4th International Conference on Cryptography, Network Security and Communication Technology (CNSCT 2025), January 17–19, 2025, Zhengzhou, China.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3723890.3723901

[*] Corresponding author

CNSCT 2025, Zhengzhou, China
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1262-3/2025/01
https://doi.org/10.1145/3723890.3723901

1 Introduction

With the rapid development of information technology in the new era, various fields of human society are increasingly dependent on the internet. However, due to the open nature of the internet, the information transmitted over public channels faces a range of security issues. Cryptographic schemes are crucial for securing internet communications. One of the most widely used internet security protocols is PAKE (Password Authenticated Key Exchange) protocol, which is user-friendly and does not require additional public key infrastructure for PAKE protocols [1]. And PAKE protocols allow parties to authenticate each other over an open channel and negotiate a shared session key by using easily memorable passwords.

Currently, most PAKE protocols are built on traditional difficult problems, such as the discrete logarithm problem and integer factorization problem [2-3]. However, with the development of quantum computing, PAKE protocols based on these traditional difficult problems are vulnerable to attacks by quantum computers. As a result, research on PAKE protocol that can withstand quantum computer attacks has become a current hot spot [4-5]. Among the cryptographic schemes resistant to quantum computing attacks, cryptographic schemes on lattice are favored due to their parallelism, efficiency, simplicity and versatility [6-7]. Therefore, cryptographic schemes on lattice are considered among the most promising post-quantum cryptography solutions for the post-quantum era [8].

For widely used PAKE protocols on lattices, user's passwords are typically stored in plaintext or as hash values on a server [9-11]. These protocols are not well-researched and suffer from low communication efficiency, with most relying on a single-server setup. If a server is compromised, there is a risk of user data leakage. To address these issues, researchers have proposed password authentication protocols based on two-server and multi-server architectures, which can resist server leakage attacks. Therefore, designing a secure and efficient lattice-based PAKE protocol in two or multi-server environments is of great significance.

To date, only a few multi-server PAKE protocols based on public key infrastructure (PKI) models for lattice-based systems exist, and these cannot be applied to two-server scenarios [5]. Moreover, multi-server architectures necessitate the use of cryptographic primitives such as digital signatures and zero-knowledge proof to ensure security, significantly increasing computational overhead [12-17]. Lattice-based multi-server PAKE protocols also require costly cryptographic primitives such as fully homomorphic encryption and secret sharing, which decrease protocol efficiency and increase communication and storage costs. On the other hand,